

**IN THE CLAIMS**

This listing of claims will replace all prior versions, and listings, of claims in the application:

1           1. (Currently Amended) A master digital data creation device for  
 2   supplying second digital data obtained by scrambling first digital data to a  
 3   digital data reproduction device having a recording medium, comprising:  
 4           an encryption block generating a first control word based on an  
 5   allowable number of reproductions specified by the digital data reproduction  
 6   device and applying a one-way function to the first control word to produce a  
 7   number of times corresponding to the allowable number of reproductions to  
 8   generate a second control word;  
 9           a scrambler receiving the second control word for scrambling the first  
 10   digital data using the second control word to produce the second digital data;  
 11   and  
 12           an output block outputting the second digital data and the first control  
 13   word to the digital data reproduction device.

1           2. (Currently Amended) A digital data reproduction device comprising:  
 2           an acceptor accepting recording media on which ~~second~~ first digital  
 3   data and a first control word  $CW_k$  are recorded, said first control word being  
 4   generated based on a specified allowable number  $k$  of reproductions, said  
 5   ~~second~~ first digital data being generated by scrambling desired ~~first~~ second  
 6   digital data using a second control word  $CW_o$  generated by applying a one-  
 7   way function to the first control word  $CW_k$   $k$  times;

a decryption block receiving the first control word  $CW_k$  and applying the one-way function to the first control word  $CW_k$   $k$  times to produce the second control word  $CW_0$ ;

a de-scrambler receiving the ~~second~~first digital data and the second control word  $CW_0$  and de-scrambling the ~~second~~first digital data using the second control word  $CW_0$  to produce the ~~first~~second digital data; and

a reproduction unit reproducing the ~~first~~second digital data generated by said de-scrambler,

wherein, after every reproduction by said reproduction unit, said decryption block writes a third control word  $CW_{(k-1)}$  back to said recording media, said third control word  $CW_{(k-1)}$  being generated by applying the one-way function to the first control word  $CW_k$  once, and wherein, if the first control word  $CW_k$  received from the recording media equals the second control word  $CW_0$ , the de-scrambling by said de-scrambler and the reproduction by said reproduction unit are inhibited.

3. (Currently Amended) The digital data reproduction device according to claim 2, wherein, when a desired number of reproductions,  $n$ , is received from some other reproduction device, said decryption block receives the first control word  $CW_k$  from the recording media and, if  $k \geq n$ , applies the one-way function to the first control word  $CW_k$   $(k-n)$  times to produce the third control word  $CW_n$  and applies the one-way function to the first control word  $CW_k$   $n$  times to produce the fourth control word  $CW_{(k-n)}$ ; and records the fourth control word  $CW_{(k-n)}$  on the recording media for updating, further comprising:

9            an output block outputting the ~~second~~first digital data recorded on the  
10    recording media, and the third control word  $CW_n$ , obtained from the decryption  
11    block, to the other reproduction device.